Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Peter Schaar
Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-[redacted]
TELEFAX (0228) 997799-[redacted]
E-MAIL ref6@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 18.09.2013

BARMER GEK
Hauptverwaltung
Postfach 200108
42271 Wuppertal

nachrichtlich:

Bundesversicherungsamt
Friedrich-Ebert-Allee 38
53113 Bonn

Bundesministerium für Gesundheit
53107 Bonn

BETREFF **Datenschutzrechtlicher Beratungs- und Kontrollbesuch bei der BARMER GEK in Wuppertal vom 28. und 29 August 2013**
BEZUG Mein Ankündigungsschreiben vom 16. August 2013

Sehr geehrte Damen und Herren,

am 28. und 29. August 2013 haben meine Mitarbeiter Herr RD [redacted] und Herr RR Dr. [redacted] einen datenschutzrechtlichen Beratungs- und Kontrollbesuch im System-haus gkv Informatik der BARMER GEK nach §§ 24 Abs. 1 und 26 Abs. 3 Bundesdatenschutzgesetz (BDSG) durchgeführt. Für die freundliche Aufnahme meiner Mitarbeiter und die offene Gesprächsatmosphäre möchte ich mich bedanken.

Schwerpunkt des Besuchs war die Prüfung des Card Management Systems (CMS) für die elektronische Gesundheitskarte der BARMER GEK, insbesondere die Datenschutzorganisation einschließlich technischer und organisatorischer Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit beim Umgang mit Versichertendaten und Gesundheitsdaten.

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

Im Einzelnen führte der Besuch zu den folgenden Feststellungen:

A. Datenverarbeitung und Verantwortlichkeiten

Die gkv Informatik (im folgenden gkvi) verarbeitet die Versichertendaten für die BARMER GEK und für andere Kassen. Dabei ist die gkvi als Auftragnehmer der BARMER GEK tätig und betreibt in Wuppertal zwei Rechenzentren (RZ) inklusive Hochsicherheitsbereichen. Der Beratungs- und Kontrollbesuch fand am Standort Lichtscheid statt. Die gkvi besitzt eigene Unterauftragnehmer, beispielsweise einen Dienstleister für die Wartung.

Ein Gesellschaftervertrag regelt, welche Prozesse und Daten bei der BARMER GEK verbleiben. Die gesamte Datenverarbeitung der BARMER GEK wird durch die gkvi abgewickelt. So liegen bei der gkvi sämtliche Versichertendaten und Bilder (Fotos) der Versicherten.

Die BARMER GEK arbeitet mit verschiedenen Dienstleistern zusammen, beispielsweise für die Produktion der eGK. Die im Rahmen von Ausschreibungsverfahren vergebenen Leistungsbeschreibungen enthalten nach Aussagen der BARMER GEK die relevanten datenschutzrechtlichen Vorgaben und werden nach Auftragsvergabe und Anpassung an die aktuelle Gesetzeslage Vertragsbestandteil.

Der Auftrag der BARMER an die gkvi für das CMS konnte meinen Mitarbeitern nicht vorgelegt werden. Auch die Verträge über die Auftragsdatenverarbeitung (§ 11 BDSG) mit dem Dienstleister der BARMER GEK (PAV Card, Morpho Cards GmbH, siehe Abschnitt B.I.) und der gkvi (Wartung) konnten uns nicht bzw. nur teilweise vorgelegt werden.

Ich bitte um vollständige Nachreichung der zuvor genannten Unterlagen bis zum 18.12.2013.

Nach § 80 SGB X Abs. 3 hat die BARMER GEK vor der Auftragserteilung die beabsichtigte Beauftragung der Aufsichtsbehörde mitzuteilen. Deswegen ist es schwer verständlich, warum zum Zeitpunkt der Kontrolle kein Vertrag zur Einsicht vorgelegt werden konnte.

Ich bitte mir deshalb mitzuteilen, wann das Bundesversicherungsamt als Aufsichtsbehörde von der Beauftragung in Kenntnis gesetzt wurde (bitte Übersendung einer Kopie des Schreibens). Weiter bitte ich um Vorlage der vollständigen Auftragserteilung(en) bis zum 18.12.2013.

B. Erstellung und Verwaltung der elektronischen Gesundheitskarte (eGK)

Die gkvi betreibt die Telematik-Infrastruktur und die Systeme zur Ausgabe der eGK für die AOK und die BARMER GEK. Sie verwaltet sämtliche die eGK betreffenden Prozesse und die Daten der Versicherten.

Hierzu betreibt die gkvi vier Fachdienste: einen Update Flag Service (UFS), das CMS, einen Versichertenstammdaten-Dienst (VSDD) sowie ein Karten- und Applikationsmanagementsystem (KAMS) für die Produktion der eGKs.

I. Ausgabe der eGK

Im Gespräch wurde meinen Mitarbeitern der Ausgabeprozess der eGK an die Versicherten vorgestellt. Die eigentliche Herstellung der eGK verbleibt bei der BARMER GEK. Diese arbeitet hierfür mit zwei Dienstleistern (Unterauftragsnehmer der BARMER GEK) zusammen, der PAV (Paul Albrecht Verlag) Card als Digitalisierer und der Morpho Cards GmbH als Personalisierer. Die in diesem Zusammenhang relevanten Sicherheitshandbücher für den Datenschutz wurden meinen Mitarbeitern vorgelegt.

Für die Herstellung der Karte ist es zunächst notwendig, dass der Versicherte ein Bild von sich einreicht. Dabei werden nur Bilder von Personen zugelassen, die auch angeschrieben wurden. Es existieren drei Wege für die Bildeinreichung:

1. postalisch;
2. per Upload mittels MMS oder Internet (Identitätsprüfung mittels Geburtsdatum und Ziffer auf dem Anschreiben);
3. per Übergabe in einer Geschäftsstelle der BARMER.

Nachfolgend wird das Bild den oben genannten Dienstleistern zur Verfügung gestellt. Das fertige Bild wird im VSDD gespeichert und mittels Zertifikatsschutz im CMS hinterlegt. Nach sechs Monaten erfolgt die vollständige Löschung von Bild und Antrag. Dies ist in den Verträgen mit den Dienstleistern so vereinbart.

Im Stammdatenhaltungssystem wird das Bild ausschließlich zum Zwecke der Kartenproduktion weiterhin gespeichert. Bittet der Versicherte um Löschung, wird dieser Bitte entsprochen und ein Hinweis auf Neueinreichung im VSDD hinterlegt. Bei Austritt aus der Versicherung oder Tod des Versicherten greifen entsprechende Löschroutinen, die Zertifikate sollen maximal fünf Jahre nach Ende der Kartengültigkeit gelöscht werden.

II. (Un-)Berechtigter Zugriff auf die eGK

Gemäß gkvi soll das CMS zukünftig den Zugriff auf die eGK durch die angeschlossenen Arztpraxen steuern. Wenn ein Versicherter seine eGK in einen Kartenleser platziert, so prüft diese, ob es zu Änderungen bei den persönlichen Daten gekommen ist und aktualisiert diese. Für diesen Fall ist der UFS vorgesehen. Dabei müssen zwei Fälle unterschieden werden:

- Update der Stammdaten – in diesem Fall erfolgt ausschließlich ein Zugriff auf den VSDD.
- Update der Anwendungen – in diesem Fall erfolgt ein Zugriff auf das CMS. Dieser Fall wird aber gemäß Aussagen der gkvi-Mitarbeiter selten eintreten.

Durch eine zukünftige Schemaänderung des VSDD wird sichergestellt, dass bestimmte Attribute auf der eGK in einem geschützten Container abgelegt werden müssen, erfolgt.

III. Vernichtung der eGK

Für die Produktion der eGK werden X.509 Zertifikate verwendet. Die Zertifizierungsstelle wird außerhalb des Rechenzentrums durch einen zugelassenen Dienstleister betrieben, im Falle der BARMER GEK das Trustcenter der Atos Origin GmbH.

Nach Auskunft der gkvi wird im Falle eines Verlusts der eGK ein Sperrsatz an den Trusted Service Provider übermittelt. Nachfolgend wird eine neue eGK mit dem zuvor eingereichten Bild an den Versicherten übersandt. Bei einem Umzug erfolgt der Versand einer neuen Karte mit der Bitte um Zerstörung der alten. Da diese Zerstörung nicht garantiert werden kann, wird ebenfalls zusätzlich ein Sperrsatz an den Trusted Service Provider versandt.

Die Daten der alten eGKs verbleiben gemäß der Aussagen der gkvi weiterhin im System, da die Karte noch physisch vorhanden sein könnte. Zertifikatsdaten werden 5 Jahre gespeichert.

IV. Change Management

Die gkvi bezieht ihre Software von der AOK Systems GmbH. Um die Mandantenfähigkeit der Software zu gewährleisten, werden kassenspezifisch zusätzliche Funktionen zur Verfügung gestellt.

Meine Mitarbeiter haben bei der Kontrolle darauf hingewiesen, dass die BARMER GEK durch die gkvi über wesentliche Systemupdates informiert werden sollte. Eine Freigabe der aktuellen Version muss durch die BARMER GEK erfolgen. Ins-

besondere muss ein revisionsfähiger Change-Management-Prozess implementiert werden, bei dem jede Softwareversion eingefroren wird und der letzte Stand prüfbar ist.
Am zweiten Tag der Kontrolle wurden meinen Mitarbeitern Unterlagen zum Change Management vorgelegt. Sie wurden darüber informiert, dass regelmäßige Meetings zwischen Mitarbeitern der BARMER GEK und der gkvi stattfinden, in denen über wesentliche Softwareänderungen berichtet wird und neue Versionen durch die BARMER GEK freigegeben werden.

Das Change Management sollte dahingehend geändert werden, dass wesentliche Änderungen schriftlich festgehalten werden und ein einem offiziellen Verfahren durch die BARMER GEK freigegeben werden. Nur so ist das Gesamtsystem auch effizient revisionsfähig. Die Durchsicht sämtlicher Besprechungsprotokolle reicht für diesen Zweck nicht.

C. Technische und organisatorische Kontrolle vor Ort

I. Videoüberwachung

Weite Teile des Geländes der gkvi werden videoüberwacht. Nach Aussagen eines Mitarbeiters der gkvi werden die entsprechenden Daten 36 Stunden gespeichert und dann gelöscht.

Insgesamt befinden sich auf dem Gelände jedoch nur drei Piktogramme, die diese Videoüberwachung kenntlich machen. Diese Piktogramme sind darüber hinaus so angebracht, dass nicht alle Besucher sie bewusst wahrnehmen können.

Es wird empfohlen, im gesamten Gebäude und auf dem Gelände entsprechende Hinweise auf die Videoüberwachung anzubringen, insbesondere an Schleusentüren und an Orten, an denen die Videoüberwachung stattfindet.

II. Zutrittsberechtigungen

Die zentralen Informationsverarbeitungseinrichtungen der gkvi befinden sich innerhalb des Hochsicherheitsbereiches. Der Zugang hierzu wird durch ein Berechtigungskonzept und die Ausgabe von Schlüsselkarten geregelt. Berechtigungen werden in der Regel permanent (Zutrittsberechtigung im Zutrittsystem eingestellt) oder temporär (Erlöschen nach einem Kalendertag) eingeräumt. Für die Vergabe der Berechtigungen sind die Bereichsleiter und Fachbereichsleiter der gkvi zuständig.

Meinen Mitarbeitern wurde eine Liste aller Zutrittsberechtigungen von externen Mitarbeitern vorgelegt. Die Liste führt namentlich die Verantwortlichen für die Vergabe der Zutrittsberechtigungen und die Begründungen auf. Insbesondere findet keine Löschung von Mitarbeitern aus Berechtigungslisten statt. So sind dort teilweise Mitarbeiter mit temporären Berechtigungen („t“) vermerkt, die diese bereits seit über einem Jahr nicht mehr besitzen. Für die temporären Berechtigungen bitte ich daher sicherzustellen, dass die Liste aktuell gehalten wird und abgelaufene Zutrittsberechtigungen gelöscht werden.

Die Ausgabe der Zutrittsberechtigungen erfolgt mittels einer Schlüsselliste (Zutrittsbuch). Hierzu werden nach Prüfung des Dienstausweises bzw. des Personalausweises Zutrittskarten vergeben.

In der Schlüsselliste werden alle Mitarbeiter der gkvi sowie alle externen Mitarbeiter wie die der BARMER GEK, des Servicepersonals oder der Dienstleister aufgeführt. Mitarbeiter der BARMER haben ohne Zutrittsberechtigung keinen Zugriff auf das CMS und keinen Zutritt zu den Systemen. In der Liste wird die Ausgabe der Zutrittskarten protokolliert. Die Liste wird über einen Zeitraum von einem Jahr verwahrt.

Meinen Mitarbeitern ist bei der Kontrolle aufgefallen, dass zu einzelnen Beschäftigten personenbezogene Daten wie „Urlaub“ oder „Krankheit“ in der Schlüsselliste vermerkt werden. Ich empfehle, nicht notwendige personenbezogene Merkmale aus der Schlüsselliste zu entfernen und diese in Zukunft dort nicht einzutragen bzw. nur allgemeine Hinweise wie beispielsweise „abwesend“ vorzunehmen.

Gemäß Abschnitt 5.3.4 des Dokuments „Richtlinie 13 - Zutritt zu Hochsicherheitsbereichen am Standort Wuppertal“ müssen externe Mitarbeiter für eine temporäre Zutrittsberechtigung ihren Personalausweis hinterlegen. Dieser wird von der Sicherheitszentrale zudem kopiert. Es darf jedoch laut § 1 Abs. 1 S. 3 des Personalausweisgesetzes von Inhabern des neuen Personalausweises nicht mehr verlangt werden, den Personalausweis als Sicherheit zu hinterlegen oder aus sonstigen Gründen aus der Hand zu geben. Um die Rückgabe der Zutrittskarten sicherzustellen, sollte daher anstelle des Hinterlegens und Ablichtens des Personalausweises ein anderes Konzept erarbeitet und in der Richtlinie verankert werden.

Nach Aushändigung der Zutrittskarte erfolgt der Eintritt in den Hochsicherheitsbereich durch eine Vereinzelungsschleuse. Wie meine Mitarbeiter festgestellt haben, schließt diese bei Eintritt von mehreren Personen erst nach 45 Sekunden. Daher wird empfohlen, dass beim Zutritt zum Hochsicherheitsbereich der letzte

Mitarbeiter (Inhaber der Karte) solange an der Schleuse wartet, bis diese geschlossen wurde. Dies sollte auch im Sicherheitskonzept verankert werden.

Innerhalb des Hochsicherheitsbereiches erfolgt ein Zugang in den eGK-Käfig durch 4-Augen-Prinzip (Zutrittskarte und biometrische Authentisierung). Der Zutritt wird protokolliert. Die zentralen Komponenten wie die Hardware Security Modules (HSM) befinden sich innerhalb des Käfigs. Der Käfig ist speziell gegen Elementarereignisse geschützt.

Im Rechenzentrum existiert zudem ein Tresor mit drei Chipkarten für die HSMs. Auch hier wird der Zutritt entsprechend protokolliert.

Entsprechende Unterlagen zum Zutritt zu den Hochsicherheitsbereichen und dem Umgang mit den Tresoren wurden meinen Mitarbeitern ausgehändigt.

Das Sicherheitssystem entspricht den datenschutzrechtlichen Anforderungen. Die Maßnahmen begrüße ich sehr.

III. Rollensystem

Die Zuordnung von Mitarbeitern der gkvi zu verschiedenen Berechtigungen erfolgt durch ein meinen Mitarbeitern vorgelegtes Rollenkonzept. Gemäß Rollenzuordnung besitzen ca. 80 Mitarbeiter der gkvi mindestens eine Rolle. Rollen werden über die Personalabteilung beantragt und durch Fachbereichsleiter vergeben und entzogen. Eine Matrix dokumentiert die sich gegenseitig ausschließenden Rollen.

Die Zuständigkeit der Mitarbeiter der gkvi unterscheidet sich nicht nach Krankenkassen. Rollen werden nur für Mitarbeiter der gkvi und nicht für externe Mitarbeiter vergeben, also auch nicht für solche der BAMER GEK.

Bei Durchsicht der Datenbank sind meinen Mitarbeitern Einträge aufgefallen, die dokumentieren, dass Mitarbeitern bestimmte Rollen entzogen wurden oder sie diese nicht erhalten haben. Da die Vergabe von Rollen beispielsweise an ein eintragungsfreies Führungszeugnis gekoppelt ist, stellen diese Informationen negative Merkmale dar. Die Datenbank hat nur den Zweck der Umsetzung des Rollenkonzepts und dient nicht zur Verwaltung von Personalangelegenheiten. Diese sollten im Fachbereich Personal verwaltet werden. Die Herausnahme oder Nichtübernahme im Rollenkonzept sollte möglichst neutral behandelt werden und nicht zur Stigmatisierung der Mitarbeiter führen. Daher empfehle ich, diese Einträge aus der Datenbank zu entfernen. Der Hinweis auf die erforderliche Dokumentati-

on von eintragsfreien Führungszeugnissen im Sicherheitskonzept (S. 44) sollte angepasst werden.

IV. Benutzerverwaltung

Im Rahmen der Besichtigung eines Mitarbeiterbüros wurde die Netzwerkinfrastruktur und die Benutzerverwaltung vorgestellt.

Das heterogene Netzwerk besteht aus drei Komponenten, einem Windows-System, einem Linux-System und einem AIX-System (Betriebssystem für die HSMs). Auf den Systemen wird zwischen verschiedenen Benutzerkonten unterschieden, es liegt kein Domänenkonzept vor. Die verschiedenen Rollen, wie z.B. die für Systemadministratoren, werden spezifisch für die jeweiligen Systeme vergeben.

Das derzeitige System ist nicht revisionsfähig, da drei verschiedene Systeme geprüft und abgeglichen werden müssen. Dies wurde im Gespräch durch Herrn XXXXXX bestätigt. Nach derzeitigem Stand können beispielsweise Rechte von einem System zu einem anderen portiert werden. Dort können weitere Rechte zugeschaltet und neue User eingerichtet werden. Insbesondere passen die Rollen des Rollenkonzeptes nicht immer zu den Berechtigungen im Windows System. So trennt das Windows-System beispielsweise nicht zwischen den Rollen „DB-Admin“ und „KAMS-Admin“.

Ich halte es daher für erforderlich, für die gesamte Netzwerkinfrastruktur ein Konzept vorzusehen, das zumindest eine Revisionsfähigkeit für das Rollenkonzept des gesamten Systems vorsieht.

Eine Überprüfung von Benutzerkennungen muss relativ einfach und übersichtlich vorgenommen werden können. Den Einsatz einer entsprechenden Verwaltungssoftware würde ich begrüßen.

Nach Angaben der gkvi existieren im System keine Gast-Kennungen oder Kennungen externer Mitarbeiter.

Passwörter müssen alle 90 Tage neu vergeben werden, dabei sind die letzten 10 Passwörter ausgeschlossen. Ein Passwort muss Klein-/Großbuchstaben, Zahlen und Sonderzeichen enthalten, die gesamte Passwortrichtlinie ist im Sicherheitskonzept dokumentiert. Meine Mitarbeiter haben darauf hingewiesen, dass eine zwingende Einschränkung des Adressraums für die Passwörter ungünstig ist und darauf verzichtet werden sollte.

Eine Software „KeyPass“ (Passwortsafe mit Masterpasswort) ermöglicht für Nutzer mit mehreren Passwörtern den Zugriff auf ihre Passwörter.

Die Urlaubsvertretung wird durch einen Abwesenheitsassistent geregelt. Der Zugriff auf fremde Postfächer ist nicht erlaubt.

Für die Datensicherung erfolgt eine regelmäßige Sicherung im Haus mit einer Ausnahme: Der Masterschlüssel für die Ableitung der Schlüssel ist bei einer Bank verwahrt.

Derzeit gibt es keine Telearbeiter. Mobile Arbeiter nutzen VPN und entsprechende Security Token. Der Zugriff auf die Telematik ist für mobile Arbeiter nicht möglich.

V. Protokolldaten und Aufbewahrungsfristen

Gemäß Abschnitt 16 des Sicherheitskonzeptes werden sicherheitsrelevante Protokolle und Dokumente 6 Monate nach ihrer Löschung im File-System auch in den Backup Systemen gelöscht und „*mindestens entsprechend den gesetzlichen Regelungen*“ aufbewahrt. Ich empfehle, diese Aufbewahrungsdauer im Sicherheitskonzept explizit zu nennen.

Nach Angaben der gkvi sind sämtliche Logdateien auf Name-Servern in der Hochsicherheitsumgebung hinterlegt. Zur Auswertung der Protokolldaten finden sich im Sicherheitskonzept keine Angaben. Hier sollte ergänzt werden, wer in welchen Zyklen die Auswertung vornimmt und wann diese gelöscht werden.

Nach der Kontrolle wurde meinen Mitarbeitern ein umfangreiches Sicherheitskonzept vorgelegt. Dies begrüße ich.

D. Sonstiges

VI. Intrusion Detection / sicherheitsrelevante Ereignisse

Laut Aussagen der Mitarbeiter der gkvi und der BARMER GEK erfolgt bei sicherheitsrelevanten Ereignissen eine Unterrichtung seitens der gkvi an die BARMER GEK. Außerdem finden regelmäßige Abstimmungen und Meetings statt.

Entsprechende Unterlagen (Einstufungskriterien für Security Incidents) wurden meinen Mitarbeitern zu Verfügung gestellt.

Im Abschlussgespräch wurde von der gkvi zugesagt, die zuvor genannten Empfehlungen umzusetzen.

Zu den oben im Einzelnen dargelegten Punkten bitte ich um Stellungnahme bis zum 18.12.2013.

Mit freundlichen Grüßen

Schaar